📘 **Reference Guide: Identifying Phishing Emails and Email-Based Malware**
Audience: Cybersecurity professionals and company email users
Purpose: Help identify suspicious emails and prevent security breaches
Author: Thi Nguyen
Date: 07/09/2025

📬 SECTION 1: For General Email Users (Non-Technical Staff)

🔍 Common Signs of Phishing Emails:

1. **Urgent or Threatening Language**
   Example: “Your account will be deactivated in 24 hours!”
   ➤ Don’t panic. Real companies don’t use threats.

2. **Unknown or Fake Sender**
   Example: `security@gmaill.com` instead of `security@gmail.com`
   ➤ Check the sender’s email carefully.

3. **Suspicious Links**
   Tip: Hover over a link before clicking.
   ➤ If the link looks unfamiliar or mismatched, don’t click.

4. **Unexpected Attachments**
   Warning: Attachments with `.exe`, `.zip`, or `.docm` (macros) may be malware.
   ➤ Only open attachments from trusted sources.

5. **Requests for Private Info**
   Example: Asking for your password or bank info.
   ➤ Never share personal or company info via email.

🛡️ SECTION 2: For Cybersecurity Professionals

🧠 Technical Indicators of Phishing or Malware:

- **Mismatch in Header Fields**
  ➤ If “Reply-to” differs from the “From” address, it could be spoofed.

- **Embedded Scripts**
  ➤ Look for hidden JavaScript in HTML emails.

- **User Pattern Alerts**
  ➤ Multiple reports of the same email can signal a phishing campaign.

- **Malicious Hashes or IPs**
  ➤ Scan suspicious attachments with VirusTotal or hybrid-analysis.

- **Macro Payloads**
  ➤ Flag `.doc` or `.xls` files that request macro access.

✅ Quick Response Guide

Situation	What to Do
Suspicious email received	Don't click or reply. Report to IT/Security.
Opened malicious attachment	Disconnect from Wi-Fi. Contact Security Ops.
Unsure if email is legitimate	Ask your IT team before interacting.

🛠️ Tips for Both Staff & Security Teams

- Use email filters and spam protection.
- Provide regular cybersecurity training.
- Encourage a "pause and check" culture before clicking.

📌 *This guide was created as part of the Google Cybersecurity Certificate assignment using the TCREI prompting framework and generative AI assistance.*